UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/701,154	11/03/2003	Massimiliano Antonio Poletto	12221-014001	5561

26161 7590 01/29/2007

FISH & RICHARDSON PC
P.O. BOX 1022
MINNEAPOLIS, MN 55440-1022

EXAMINER	
MEHRMANESH, ELMIRA	
ART UNIT	**PAPER NUMBER**
2113	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	01/29/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/701,154	POLETTO ET AL.	
	Examiner	Art Unit	
	Elmira Mehrmanesh	2113	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03 November 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-24* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-24* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *03 November 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This action is in response to an amendment filed on November 03, 2006 for the application of Poletto et al., for a "Connection based anomaly detection" filed November 3, 2003.

Claims 1-24 are presented for examination.

Claims 23-24 are rejected under 35 USC § 102.

Claims 1-22 are rejected under 35 USC § 103.

Claims 1-4, 6-7, 14-16, and 24 have been amended.

Double Patenting

The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., In re Berg, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); In re Goodman, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); In re Longi, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); In re Van Ornum, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); In re Vogel, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and In re Thorington, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

Claims 8-13, and 17-22 are provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 5-10 of copending Application No.10701356. Although the conflicting claims are not identical, they are not patentably distinct from each other, please refer to the previous Office action mailed on May 05, 2006 for the double patenting rejection details.

Examiner notes that applicant has responded in the Remarks filed November 03, 2006 they will consider timely submission of a terminal disclaimer in compliance with 37 CFR 1.321 (c) or 1.321 (d) to overcome the rejection upon indication of allowable subject matter.

Claim Rejections - 35 USC § 101

In response to amendments to claim 24, the last rejection has been withdrawn.

Claim Rejections - 35 USC § 112

In response to claim 24, the applicant's remarks have been fully considered and the last rejections have been withdrawn.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

Claims 1-5, 12-16, and 21-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Malan et al. (U.S. PGPUB No. 20020032871) in view of Cidon et al. (U.S. Patent No. 6,269,330).

As per claim 1, Malan discloses a system, comprising:

a plurality of collector devices that are disposed to collect packets that are sent between nodes on a network (page 5, paragraph [0066]) and (Fig. 4, elements 20, 20b).

an aggregator (page 5, paragraph [0071], lines 7-11) and (page 3, paragraphs [0032], [0033], and [0034]) that receives network data from the plurality of collector devices (Fig. 4, element 20, 20b).

Malan fails to explicitly disclose a connection table.

Cidon teaches:

sending connection information to identify host connection pairs from collected (col. 14, lines 64-67 through col. 15, lines 1-10)

producing a connection table (Fig. 3, element 154) that maps each node of a network to a record object that stores information about traffic to or from the node (col. 14, lines 64-67 through col. 15, lines 1-10).

It would have been obvious to one of ordinary skill in the art at the time the invention to use the method of network fault location of Cidon et al.'s in combination with the network anomaly detection system of Malan et al. to effectively detect network anomalies.

One of ordinary skill in the art at the time the invention would have been motivated to make the combination because both inventions disclose a method of blocking Denial of Service Attacks in a network. Malan et al. discloses a system to detect and block DoS attacks by collecting network data statistics (page 3, paragraph [0028] and [0029]). Cidon et al. discloses of a traffic generator that generates network traffic and a traffic analyzer to analyze the traffic statistics to locate network faults (Fig. 2).

As per claim 2, Malan discloses the aggregator determines occurrences of network events (page 5, paragraph [0071] and page 3, paragraph [0032])

Cidon teaches:

at least in part from the connection patterns derived from the connection table (col. 14, lines 64-67 through col. 15, lines 1-10) and (Fig. 5, *evaluate performance of network*).

As per claim 3, Malan discloses the aggregator further comprises: a process that collect statistical information on packets that are sent between nodes on a network and which sends the statistical information to the aggregator (page 6, paragraph [0075], lines 8-13 and page 7, paragraph [0086], lines 1-10).

As per claim 4, Malan discloses the aggregator device further comprises:

a process to aggregate detected anomalies into the network events (page 5, paragraph [0071] and page 3, paragraph [0032]).

Cidon teaches:

a process to detect anomalies in connection patterns (col. 14, lines 64-67 through col. 15, lines 1-10) and (Fig. 5, *evaluate performance of network*).

As per claim 5, Malan discloses the collectors have a passive link to devices in the network (FIG. 7).

As per claims 12 and 21, Cidon discloses the connection table (Fig. 3, element 154) includes a plurality of connection sub-tables (col. 5, lines 23-24, *nodal tables*) to track data at different time scales (col. 14, lines 64-67 through col. 15, lines 1-10).

As per claims 13 and 22, Cidon discloses the connection sub-tables (Fig. 3, element 154) and (col. 5, lines 23-24, *nodal tables*) include a time-slice connection table that operates on a small unit of time and at least one other sub-

table that operates on a larger unit of time than the time slice sub-table with each sub-table holding the sum of records received from all collectors during respective units of time (col. 14, lines 64-67 through col. 15, lines 1-10).

As per claim 14, Malan discloses a method, comprises:

A plurality of collector devices (Fig. 4, elements 20, 20b) to an aggregator (page 5, paragraph [0066])

Malan fails to explicitly disclose a connection table.

Cidon teaches:

sending connection information to identify host connection pairs from collected (col. 14, lines 64-67 through col. 15, lines 1-10)

producing a connection table (Fig. 3, element 154) that maps each node of a network to a record object that stores information about traffic to or from the node (col. 14, lines 64-67 through col. 15, lines 1-10).

As per claim 15, Malan discloses collecting statistical information in the collector devices to send to the aggregator device (page 5, paragraph [0071]).

As per claim 16, Malan discloses determining occurrences of network anomalies (Fig. 5, element 20b) aggregating anomalies into the network events and communicating occurrences of network events (Fig. 5, element 20b) to an operator (page 6, paragraph [0075], lines 8-13).

Claims 6 and 7 are rejected under 35 U.S.C. 103(a) as being unpatentable over Malan et al. (U.S. PGPUB No. 20020032871) in view of Cidon et al. (U.S. Patent No. 6,269,330) and further view of Hill et al. (U.S. Patent No. 6,088,804).

As per claim 6, Malan discloses the anomalies include denial of service attacks (page 4, paragraph [0057]).

Malan et al. fails to explicitly disclose scanning attacks.

Hill teaches:

the anomalies include and scanning attacks (col. 4, lines 35-41).

As per claim 7, Malan et al. fails to explicitly unauthorized access and worm propagation.

Hill teaches:

the anomalies include unauthorized access and worm propagation (col. 5, lines 57-65).

It would have been obvious to one of ordinary skill in the art at the time the invention to use the network security attack detection system of Hill et al.'s in combination with the network anomaly detection system of Malan et al. to effectively detect network anomalies.

One of ordinary skill in the art at the time the invention would have been motivated to make the combination because both inventions disclose a method of blocking security attacks in a network. Malan et al. discloses a system to detect and block DoS attacks by collecting network data statistics (page 3,

paragraph [0028] and [0029]). Hill et al. discloses a method and system to respond to security attacks by collecting data through security agents (col. 3, lines 17-30 and col. 4, lines 53-61).

Claims 8-11 and 17-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Malan et al. (U.S. PGPUB No. 20020032871) in view of Cidon et al. (U.S. Patent No. 6,269,330) and further view of Chi et al. (U.S. Patent No. 5,940,870).

As per claims 8 and 17, Cidon discloses the connection table (Fig. 3, element 154)

Malan in view of Cidon fails to explicitly disclose indexing by address.

Chi teaches:

includes a plurality of records that are indexed by source address (col. 5, lines 29-43).

It would have been obvious to one of ordinary skill in the art at the time the invention to use the network anomaly detection system of Malan et al. in combination with the translating address method of Chi et al.'s to effectively address mapping tables of a multi-computer cluster.

One of ordinary skill in the art at the time the invention would have been motivated to make the combination because both inventions disclose a method of blocking security attacks in a network. Malan et al. discloses a database for recording source and destination of packet flows in the network (page 5,

paragraph [0067]). Chi et al. discloses a mapping table that stores the source and destination information of the network nodes (Fig. 8). Network statistical information is used to efficiently identify the source and destination nodes of the network (Chi, col. 3, lines 33-37) and (Malan, page 5, paragraph [0067], lines 10-14).

As per claims 9 and 18, Cidon discloses the connection table (Fig. 3, element 154)

Chi teaches:

includes a plurality of records that are indexed by destination address (col. 5, lines 29-43).

As per claims 10 and 19, Cidon discloses the connection table (Fig. 3, element 154)

Chi teaches:

includes a plurality of records that are indexed by time (col. 5, lines 29-43).

As per claims 11 and 20, Cidon discloses the connection table (Fig. 3, element 154)

Chi teaches:

includes a plurality of records that are indexed by source address, destination address and time (col. 5, lines 29-43).

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claim 23-24 are rejected under 35 U.S.C. 102(e) as being anticipated by Belissent (U.S. Patent No. 6,789,203).

As per claim 23, Belissent discloses a method of detecting a new host connecting to a network comprises:

receiving statistics collected from a host in the network (Fig. 6) and indicating to a console that the host is a new host if, during a period of time T, the host transmits at least N packets and receives at least N packets, and if the host had never transmitted and received more than N packets in any previous period of time with a duration of T (col. 4, lines 9-20 and col. 5, lines 62-67 through col. 6, lines 1-17). Belissent discloses a system for monitoring connection request rates over a period of time and a rejection threshold.

As per claim 24, Belissent discloses a method of detecting a failed host in a network comprises:

determining if both a mean historical rate of server response packets from a host is greater than M, and a ratio of a standard deviation of historical rate of server response packets from the host to a mean profiled rate of server response packets from the host is less than R over a period of time; and indicating the host as a potential failed host if both conditions are present (col. 4, lines 9-20 and col. 5, lines 62-67 through col. 6, lines 1-17).

Response to Arguments

Applicant's arguments have been fully considered with the examiner's response detailed below.

Applicant's arguments see pages 6-14, filed November 03, 2006 with respect to the rejection(s) of claim(s) 1-24 have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made over Malan et al. (U.S. PGPUB No. 20020032871) in view of Cidon et al. (U.S. Patent No. 6,269,330) and Chi et al. (U.S. Patent No. 5,940,870) and Belissent (U.S. Patent No. 6,789,203) in further view of Hill et al. (U.S. Patent No. 6,088,804). Refer to the corresponding section of the claim analysis for details.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Elmira Mehrmanesh whose telephone

number is (571) 272-5531. The examiner can normally be reached on 8-4:30 M-F.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Robert W. Beausoliel can be reached on (571) 272-3645. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).